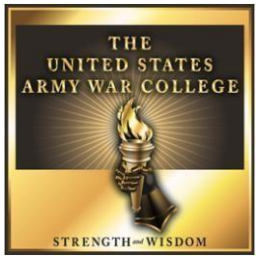
Strategy Research Project

Protecting Critical Infrastructure: A Team Sport

by

Lieutenant Colonel Carl Lamar Parsons
United States Army



United States Army War College
Class of 2015

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-04-2015	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Protecting Critical Infrastructure: A Team Sport

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Carl Lamar Parsons
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel Timothy Frantz
Department of Military Strategy, Planning, and Operations

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5504

14. ABSTRACT

Defending critical infrastructure against attack is vital to the National Security of the United States and is essential to maintaining national economic prosperity. As a symbol and instrument of national power, the U.S. military plays a broad role to protecting and defending the homeland. The military must be prepared and ready to execute homeland defense tasks and provide support to other agencies to protect critical infrastructure. To mitigate the risks to our critical infrastructure, the military, in cooperation and collaboration with other governmental agencies, must maintain a robust defense and protection plan. This paper does not advocate large overt security measures. Instead, it emphasizes the continued importance of defending the Nation's critical infrastructure by showcasing the layers of complexity and interagency support required to conduct critical infrastructure protection. The paper will make recommendations on how to move forward on defending and protecting our critical infrastructure from a whole of government approach.

15. SUBJECT TERMS
Homeland Defense, Homeland Security

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	34	

USAWC STRATEGY RESEARCH PROJECT

Protecting Critical Infrastructure: A Team Sport

by

Lieutenant Colonel Carl Lamar Parsons
United States Army

Colonel Timothy Frantz
Department of Military Strategy, Planning, and Operations
Project Adviser

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title: Protecting Critical Infrastructure: A Team Sport

Report Date: 01 April 2015

Page Count: 34

Word Count: 5504

Key Terms: Homeland Defense, Homeland Security

Classification: Unclassified

Defending critical infrastructure against attack is vital to the National Security of the United States and is essential to maintaining national economic prosperity. As a symbol and instrument of national power, the U.S. military plays a broad role to protecting and defending the homeland. The military must be prepared and ready to execute homeland defense tasks and provide support to other agencies to protect critical infrastructure. To mitigate the risks to our critical infrastructure, the military, in cooperation and collaboration with other governmental agencies, must maintain a robust defense and protection plan. This paper does not advocate large overt security measures. Instead, it emphasizes the continued importance of defending the Nation's critical infrastructure by showcasing the layers of complexity and interagency support required to conduct critical infrastructure protection. The paper will make recommendations on how to move forward on defending and protecting our critical infrastructure from a whole of government approach.

Protecting Critical Infrastructure: A Team Sport

> Essential to our national security and economic growth, America's critical infrastructure—from our plants and pipelines to our hospitals and highways—supports the physical and virtual systems that underpin American society.
>
> —Barack Obama
> President of the United States[1]

Defending the homeland and its critical infrastructure against attack is vital to the National Security of the United States. It helps protect the American way of life and is essential to maintaining national economic prosperity. As a symbol and instrument of national power, the U.S. military[2] plays a broad role in the whole of government approach to protecting and defending the homeland. The military must be prepared and ready to execute homeland defense tasks and provide support to other agencies to protect critical infrastructure. To mitigate the risks to our critical infrastructure, the military, in cooperation and collaboration with other governmental agencies, must maintain a robust defense and protection plan.

The purpose of this paper is not to advocate large overt security measures like armed sentries, tanks, and concertina wire at every port, government building, or vital industrial plant. Instead, this narrative will educate the reader on the importance of homeland defense and emphasize the continued importance of defending the nation's critical infrastructure. It will show case the complexity of protecting critical infrastructure, some of the current risks and threats , the interagency coordination required, and the consequences of not adequately preparing. Finally, the paper will make recommendations on how to move forward on defending and protecting our critical infrastructure from a whole of government approach.

It is essential for the nation and the military to develop and rehearse defensive measures to ensure our critical infrastructure remains functional and resilient.[3] The nation's critical infrastructure is more than a list of buildings and structures. It is an extremely diverse and complex set of interconnected structures, systems and networks[4] encompassing a wide range of physical and virtual assets, and services that are necessary for America's prosperity, security, and way of life.[5]

Strategic Guidance

To understand the importance of homeland defense and protecting the nation's critical infrastructure, one must first understand our enduring national interests as outlined in the current National Security Strategy (NSS). The 2015 NSS lists the enduring national interests as: "the security of the United States and its citizens, a strong innovative and growing U.S. economy, respect for universal values at home and around the world, and a rules based international order advanced by U.S leadership."[6] Linking the nation's enduring national interests and top strategic risks guides a refined strategy on defending and protecting America.

The President stated in the NSS, "The United States government has no greater responsibility than protecting the American people"[7] and outlined the top eight strategic risks that endanger this principle. These risks and threats include economic slowdown, climate change, use of weapons of mass destruction, and "catastrophic attack on the U.S. Homeland or critical infrastructure"[8] among others. Each poise a unique challenge to the U.S.; but this paper will only address the risk to our critical infrastructure and the impacts a successful attack might have on the nation.

When analyzing the strategic risks in the NSS and the President's intent to protect the American people, it is clear that homeland defense and homeland security are priority tasks for the government to undertake. With that, the NSS gives the military a clear objective to "remain ready to deter and defeat threats to the homeland, including against missile, cyber and terrorist attacks, while mitigating the effects of potential attacks and natural disasters."[9] This mandate sets the stage for further strategic guidance on the complexity and difficulty of mitigating the strategic risks.

To be successful in this endeavor, the nation must use all the elements of national power while bringing together multiple agencies and departments. This includes the collective strength and resources of the Department of Defense (DOD) and the Department of Homeland Security (DHS). As major stakeholders in protecting and defending the nation's critical infrastructure, each department plays a unique and complementary role. Both Departments will work across a complex operational homeland environment that encompasses threats and risks from all domains: cyber, maritime, land, air, and space.[10]

The U.S. military derives its strategic guidance from several source documents to include the NSS, the National Military Strategy (NMS), Quadrennial Defense Review (QDR), the Strategy of Homeland Defense and Defense Support to Civil Authorities, Presidential Policy Directives (PPD) and other communications from the senior national leadership. This guidance is further refined and articulated in Joint Publication 3-27, *Homeland Defense*, which gives guidance to the joint force on how to conduct homeland defense (HD) operations. These strategic guidance documents provide

direction for the force to plan, allocate resources, and to collaborate/coordinate with other agencies to build cohesive strategies for HD operations.

The DOD defines HD operations as more than guarding the shores and avenues of approach from invading conventional threats. The HD mission is the overall "protection of the U.S sovereignty, territory, domestic population and critical infrastructure"[11] that requires a coordinated and collaborative approach to achieving unified action.[12] The military approaches HD from a multi-pronged approach of detecting, deterring, preventing, and defeating an adversary across multiple domains.[13] Coupled with HD operations, the DOD must provide Defense Support to Civilian Agencies (DSCA) in times of national emergencies, other special domestic events, and in the form of support to law enforcement.[14]

The Department of Homeland Security (DHS) is the lead federal agency for homeland security activities (HS) since its establishment in 2002. The DHS mission and vision is "a homeland that is safe, secure, and resilient against terrorism and other hazards."[15] The core mission of DHS is protecting the homeland and the focus of the Homeland Security Enterprise. The Homeland Security Enterprise brings together 22 other federal agencies working toward one common goal and vision.[16] The vision of a safe and secure homeland overlaps and compliments the goals of the U.S. military and the DOD. With this said, critical infrastructure protection (CIP) falls into the realm of both DOD and DHS. Depending on the situation, the DOD is the lead for HD operations and supports DHS during HS operations. To add to the complexity of CIP, both HD and HS operations may happen at the same time.[17]

According to DHS, the nation's critical infrastructure is "the backbone of our nation's economy, security and health systems…[and] that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety."[18] Linking and networking our defense and preparedness together to protect our critical infrastructure is important to the nation's resiliency. With a high level of preparedness and readiness, the nation's ability to recover if faced with a complex catastrophe greatly increases. It is part of a larger strategy for the nation to be resilient and have the ability to quickly recover from attacks, disruptions and accidents.[19]

Critical Infrastructure Protection

A common framework and definition of critical infrastructure is required when describing the complexity of CIP. As a base line, critical infrastructure consist of both physical structures and virtual means. Current joint military doctrine puts critical infrastructure into two categories. The first category is defense critical infrastructure (DCI) and the second as critical infrastructure and key resources (CI/KR).

The current JP 3-27 defines DCI as "networked assets essential to project, support, and sustain military forces and operations."[20] Assets range from information and people to real physical structures such as bridges, installations, facilities, pipelines, and other key structures.[21] DCI can include DOD owned and controlled information and real property or property owned by civilian agencies or private entities.[22] CI/KR assets are "vital to the security, governance, public health and safety, economy and public confidence" of the American people.[23] The Defense Industrial Base (DIB) is considered CI/KR and the DOD is the sector specific agency in charge of its protection.[24] The

National Infrastructure Protection plan establishes national policy for the protection of CI/KR.[25]

Presidential Policy Directive/PPD21- Critical Infrastructure Security and Resilience provides a national strategic definition of critical infrastructure. This directive provides direction, establishes policies, and assigns responsibilities for critical infrastructure security and resiliency.[26] In PPD-21, critical infrastructure is defined as a diverse and complex set of "distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both physical space and cyber space…"[27] The policy list the three strategic imperatives of CIP, the 16 sub categories of critical infrastructure with sector specific agency responsibilities, and assigns the DHS overall responsibility of coordinating, providing strategic guidance, and unity of effort for CIP. The U.S. government approach to protection of critical infrastructure is "an integrated, holistic manner to reflect the nation's infrastructures interconnectedness and interdependency." [28]

As a whole of government approach to CIP, the DOD was tasked within PPD-21 as a sector responsible agency for the DIB. The DIB includes over 100,000 defense companies, contractors and subcontractors that develop, build and maintain technology and equipment for the Department of Defense.[29] The DIB provides critical capabilities, equipment, and resources to bolster U.S. national power.[30] A challenge to managing the defense of the DIB is that some of it actually resides outside the U.S.

The DHS defines critical infrastructure as the "assets, systems and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security,

national public health or safety, or any combination thereof."[31] For the purposes of this paper, physical infrastructure defense and protection are the main focus, with the understanding that cyber and virtual defense is equally as important. In regard to multinational ownership of the nation's critical infrastructure as defined in PPD-21, this paper will not address the additional layer of complexity. Multinational ownership and location of the infrastructure opens an entire line of jurisdictional and legitimacy issues for securing and defending beyond the U.S. national borders.

Threats/Risks

The United States has enjoyed a relative level of security from conventional threats to the homeland. The U.S. is bordered by the Atlantic and Pacific Oceans to the east and west that offer a high level of protection. The U.S. shares a northern and southern contiguous border with Canada and Mexico. Each neighbor is regarded as a strong ally and relative stable partner and posing no immediate security threat in a conventional sense. However, there are some concerns about porous borders, transnational criminal organizations, and infiltration lines into the homeland from Mexico.[32]

As technology advances, these simple but effective geographical advantages are shrinking. Due to the complexities of today's homeland operational environment, the military must work closely with other agencies to maintain and improve awareness across the air, maritime, space, cyberspace, and land domains as part of the nation's CIP.[33] This includes working with the DHS, Federal Bureau of Investigations and the United States Coast Guard (USCG) to mitigate threats to the U.S. homeland by conventional and asymmetrical means.

Threats, risks, and hazards exist across a wide spectrum and must be considered when developing strategies for CIP. This section will address manmade military threats and not address other types of hazards or natural occurring events. The threats considered for this argument are generated by state and non-state actors. The HD operational environment is extremely complex considering the persistent threat of state actors' desire to gain weapons of mass destruction and ballistic missile technology.[34] It is further complicated by non-state actors, violent extremists groups, and other organizations with nefarious intentions toward the American people and way of life.

Any attack on the nation's critical infrastructure will have ripple effects across America and probably the world. If the nation's layered defense and home security apparatus is penetrated and a catastrophic attack is carried out, it will most likely have major impacts on the economy, the military, and national morale. The next few pages describe plausible scenarios outlining possible attacks on our critical infrastructure and the consequences.

Three hypothetical threats to the nation's critical infrastructure are addressed. Within each threat, this paper will draw a linkage to homeland defense, homeland security and the military's role in CIP. It will also illustrate some of the potential consequences to the nation and how it effects the enduring national security interests. The three scenarios are an attack on the electric grid, an attack on a west coast port, and a terrorist attack on a designated CI/KR asset.

The Electric Grid

The nation depends on reliable and easily accessible electricity to power everything from everyday appliances, lifesaving equipment in hospitals, to machines in industry that keep America strong. The U.S. electric power grid is the life-line to most critical infrastructure sectors, providing the power for industry and essential services[35] and is a key part to the Energy Sector of critical infrastructure. A successful attack on the grid can severely impact national security, the economy by disrupting services, supply chains, and the daily American way of life.[36]

The current electric infrastructure is extremely robust and represents one of the strengths of America. It is characterized by over 360,000 miles of power lines, 180,000 miles of high voltage lines running to and from over 6,000 power plants.[37] However, the large power transformer (LPT), with its ability to regulate voltage, is the center of gravity for the grid to function properly.[38] Since LTPs are custom built for specific users, are not interchangeable, and have an average build time from five months to several years, this critical piece of equipment could be considered the lynch pin in the electric grid.[39] Without LPTs, the grid would fail to function properly.[40] To complicate matters, the U.S has a limited ability to produce LPTs and relies heavily on international resources to meet the current demand.[41]

An electromagnetic pulse (EMP) burst triggered from a ballistic missile or nuclear device over the homeland could have devastating results. A large EMP burst of radiation in the atmosphere would rain down on electrical equipment, devices, and the electric grid causing wide spread damage.[42] The origin of the threat is irrelevant at this point. In a 2008 Congressional Research Service (CRS) report to Congress, EMP

threats were assessed as rising due to nuclear weapon and associated technology proliferation and could cause damage to the nation's security and economic prosperity.[43] The impact from a devastating EMP attack on the nation's electric grid could and have monumental second and third order affects.

According to the 2008 CRS report, to create an EMP effect over a 250 mile in diameter area only requires modest rocket capabilities to loft a device into position.[44] The resulting damage would affect most unprotected electronic equipment and the electric grid in the blast radius. Some estimations believe that a powerful enough EMP detonated high in the atmosphere over the American homeland, could damage up to 50% of the electric grid.[45]

If the electric grid goes down from an EMP strike, the economic productivity loss will be significant. A study conducted by the Sage Policy Group of Baltimore and Instant Access Networks (IAN) released in 2007 estimated that a EMP blast in the Baltimore-Washington-Richmond area would result in economic impact of approximately 7% of the nation's GDP.[46] The resulting damage could cost the economy in the neighborhood of $9-$34 billion.[47] The estimated time to repair the electric grid was conservatively estimated to be between 2.5 months and 13.5 months.[48] The resulting economic impact in the U.S. would have cascading impacts worldwide.

The loss of the electric grid poses a complex problem set not only for America at large but also would hamper "military installations, the Defense Industrial Base and our critical supply chain"[49] to conduct operations, set future theaters and to respond to a crisis. To illustrate the military importance, General Jacoby, former NORTHCOM

commander, would start his day with a wide array of reports to include anything that would impact electrical grid or other critical infrastructure.[50]

It was assessed that several nations already have the technology and capacity to launch EMP strikes against the continental United States and others are pursuing it.[51] Potential adversaries such as North Korea and Iran are actively pursuing both ballistic missile technology and nuclear weapons which threaten the national security of the U.S.[52] This current and emerging threat effects the entire defense and security apparatus and should be reason for concern as the military continues to develop and field a ballistic missile defense shield.

Protecting the homeland from an EMP attack is a significant challenge to the U.S. military. The military, as a large consumer of electricity, relies on the grid to power military installations, conduct daily operations, and power the DBI. If an EMP attack occurred, military daily operations might be effected because of an increasing reliance on technology and the advances of electronics.[53] With this type of scenario, the DOD would have the lead in defeating a missile launch but after impact would transition from HD to DSCA operations in support of recovery operations.

Sea Ports

Maritime domain awareness is an essential factor in protecting key critical infrastructure within the Transportation Systems Sector.[54] The transportation sector is at risk due to an evolving threat from terrorist and other actors.[55] The U.S. plays a large role in sustaining the world economy due to an ability to sustain international commerce through its robust transportation system. The U.S. controlled maritime domain consist of over 95,000 miles of coast line, over 360 functioning ports, 25,000 miles of waterways

and a 3.4 million mile exclusive economic zone.[56] This includes eight of the world's busiest ports contributing over $700 billion to the American economy.[57]

The nation's ports are key to the world's supply chain. A 2005 CRS report to Congress on port security, stated over 80% of the world's trade is conducted through commercial shipping with over 20% transporting through U.S. ports.[58] Furthermore, over 95% of North America's trade is done by shipping and is influenced by U.S. ports capacity to quickly process container ships.[59] With the world moving toward a just in time logistics cycle and smaller on hand inventories, any disruption to a large shipping port will have worldwide implications and cascading effects. As a relative metric, a recent five day labor dispute that shutdown the ports on the West Coast had a $4.7 billion impact on the economy.[60] If a successful attack occurred, a shutdown would likely last longer and have further reaching economic impacts.[61]

As expeditionary forces, the U.S. military relies heavily on ports to deploy equipment, supplies, and resources to contingency operations in support of Geographical Combatant Commanders. Keeping ports open is a national security interest. As of 2005, the DOD categorized at least 17 different ports as strategic deployment centers.[62] To illustrate their importance, over 90% of the equipment used during Operations Desert Storm and Desert Shield was shipped out of strategic ports. If these areas are denied, then the U.S. military will have a difficult time projecting national power around the world.[63]

The number of attack scenarios are only limited by an adversary's creativity and imagination. This paper addresses a couple of potential attack scenarios to illustrate

the complexities of defending this vital category of critical infrastructure. The 2005 CRS report on port security identified the following potential attack scenarios to Congress:

- use commercial cargo containers to smuggle terrorists, nuclear, chemical, or biological weapons, components thereof, or other dangerous materials into the United States;
- sink a large commercial cargo ship in a major shipping channel, thereby blocking all traffic to and from the port;
- attack a large ship carrying a volatile fuel (such as liquefied natural gas) and detonate the fuel so as to cause a massive in-port explosion;
- attack an oil tanker in a port or at an offshore discharge facility so as to disrupt the world oil trade and cause large-scale environmental damage;
- seize control of a ferry (which can carry hundreds of passengers) or a cruise ship (which can carry more than 3,000 passengers, of whom about 90% are usually U.S. citizens) and threaten the deaths of the passengers if a demand is not met;
- attack U.S. Navy ships in an attempt to kill U.S. military personnel, damage or destroy a valuable U.S. military asset, and (in the case of nuclear-powered ships) cause a radiological release.
- use land around a port to stage attacks on bridges, refineries located on the waterfront, or other port facilities.[64]

To counter this wide range of threats, the multiple stakeholders involved in port security and CIP must work together. Maritime HD operations and Maritime HS operations share common threads and overlapping areas of responsibility. Military maritime forces must work with the USCG to detect and stop threats as early as possible. Sea ports must be protected and defended, due to their strategic importance to the economic and military instruments of national power.

The USCG is the lead service for maritime security operations and works closely with the other sea domain forces. The USCG has unique law enforcement authorities,

is not limited by the Posse Comitatus Act, and can conduct HS activities while protecting the nation's sea ports.[65] Joint missions between the USCG and U.S. Navy can enhance the nation's ability to protect critical ports that are strategic power projection nodes and those that are critical to the world's economy.

Armed Forces (asymmetrical or conventional)

An attack on the homeland by a terrorist organization or a nation state proxy targeting a CI/KR could have a lasting impact on America. Striking the homeland and impacting the nation's critical infrastructure is compounded by the influence of extremist organizations exporting their ideologies, porous borders, and Transnational Criminal Organizations (TCO) that empower the flow of illegal commodities.[66] The threat of another 9/11 attack is still a potential scenario and should not be overlooked.

In developing the current Strategy for Home Defense and Defense Support to Civil Authorities, the DOD made several threat assumptions. These assumptions include an increase in asymmetrical and terrorist threats in the homeland as the U.S. is engaged abroad and acquiring weapons of mass destruction.[67] In 2014 DHS stated, "lone offenders and small groups acting on their own initiative and without direction of a terrorist group are among the most persistent and difficult threats to counter."[68] Through war gaming dangerous courses of action, it is plausible that a group can organize and attack a critical infrastructure site.

The DHS lists several "black swan" type events that could trigger a significant change in the security situation. The DHS said,

> substantial increase in sophistication of hostile non-state actors, such as a violent extremist group gaining the ability to launch a campaign of well-coordinated and highly organized attacks, conducted by interconnected but autonomous groups or individuals within the United States.[69]

This type of coordinated event would have major impacts on the nation's security. DOD's mission is to defeat an adversary's aggression toward the U.S. The question to ponder is the following. What triggers a military response in the homeland? Is it when local law enforcement is out gunned and overwhelmed? An attack by a known belligerent, such as ISIL, in an organized fashion poises a unique challenge to whether or not a military response is required. The consequences of a successful attack by an organized aggressor on the mainland will have larger impacts that the immediate tactical effect. Trust of the American public could wane, questioning the country's ability keep America safe. A successful attack could uncover the nation's vulnerabilities and embolden others to take action.

United States Northern Command

The Commander, United States Northern Command (USNORTHCOM) is tasked with planning, organizing and, if required, conducting HD operations within the USNORTHCOM Area of Responsibility.[70] The Area of Responsibility for USNORTHCOM includes the Continental United States, Canada, Mexico, and areas out to 500 nautical miles from the coast line.[71] The CDRUSNORTHCOM works in concert with the North American Aerospace Defense Command (NORAD) to accomplish HD missions while coordinating operations across multinational lines. USNORTHCOM works closely with the DHS and other agencies to set the conditions for HD operations by sharing intelligence, monitoring threats, and building a common operating pictures for situational awareness. USNORTHCOM also plays a major role in supporting DSCA operations in response to manmade and natural disasters.

One of NORTHCOM's primary responsibilities is to build rapport and relationships with the other agencies and partnered nation's that support HD and HS operations.[72] These relationships are crucial for a unified effort while protecting the nation's critical infrastructure and homeland. NORTHCOM continuously develops relationships with interagency groups, other departments, the National Guard and multinational partners to include Canada and Mexico to "defeat threats at a safe distance."[73]

USNORTHCOM provides early warning, missile defense, and support to civilian agencies if required. General Charles Jacoby, the former commander of NORTHCOM, when addressing the Senate Arms Service Committee said "the homeland must be appropriately resourced to protect our sovereignty, secure critical infrastructure, offer sanctuary to our citizens and provide a secure base from which we project our national power."[74] He further went on to say that the homeland is faced with multiple threats and that we cannot afford to under value the investment required to defend the homeland.[75] Building relationships, as previously stated, enhances the command's ability to carry out its HD mission.

NORAD, working in parallel with USNORTHCOM, focuses on aerospace and maritime early warnings for North America while NORTHCOM "partners to conduct Homeland Defense and Civil Support operations…to defend, protect and secure the United States and its interests."[76] OPERATION NOBLE EAGLE, an interagency, multinational coordinated and conducted combat air patrol, has flown over 62,000 sorties in support of HD.[77] This coverage and early warning thwarts possible asymmetric attacks like a hijacked commercial airliner flying into a CI/KR location or

conventional threat against airspace sovereignty. To support this daily HD mission, coordination and collaboration between the DOD, DOT, DHS and the Canadian government must occur.[78]

The 2011 NMS gives clear guidance that "our Nation's most vital interests are the safety and security of our people and territory and our way of life."[79] However, with current fiscal constraints and possible continued sequestration, the role of the military defending the homeland from attack could be diminished. The military and nation will have to assume additional risk.[80] Due to budget constraints in FY 14, the Air Force saw a drop in readiness to less than 50% for units supporting NORAD's mission[81]. This impeded the integrated strategy required to execute missions in support of the HD operations and to provide early warning of an air threat and missile threat.

Missile defense is an important pillar in HD because the threat of ballistic missiles is increasing.[82] This is a key mission to protect the American homeland and its critical infrastructure from countries like North Korea and Iran, who continue to pursue ballistic missile technology.[83] In 2013, NORTHCOM began work on increasing the nation's ballistic missile defense posture after the Secretary of Defense announced increasing the number of Ground Based Interceptors from 30 to 44.[84] This increased capacity strengthens the U.S. military's ability to defend against ballistic missiles aimed at the homeland. Even though not likely, a ballistic missile carrying a weapon of mass destruction targeting the homeland poises a significant enough risk to pursue anti-ballistic technology.

As outlined in the 2010 Ballistic Missile Defense Report, the policy of the U.S. government is "to defend the homeland from limited ballistic missile attack by a regional

actor such as North Korea or Iran."[85] The strategy is built upon a whole of government approach of dissuading, deterring, and defeating if required. To defeat an attack, the U.S. must continue its research and development and procurement of affordable ballistic missile defense technology.[86]

Recommendations

Defending the homeland in a complex and dangerous environment is a daunting task. Based upon some of the plausible threats against the homeland, the following recommendations are made. All stakeholders should continue to develop and exercise contingency plans. The military should assign a task organized HD response force to USNORTHCOM and implement a leader development program that supports HD. The U.S. government should clearly designate the difference between HD and HS missions while rehearsing transitions between interagency and military leads during operations.

The U.S. military must prepare for HD operations by understanding the complexities of the homeland operational environment. Much like preparing for a deployment overseas, all units should work in a joint interagency environment that test homeland defense skills and tasks to achieve unity of effort. The military, in conjunction with its interagency partners, should continue to build contingency plans and conduct joint combined rehearsals with all stakeholders. These rehearsals should take place on or in close proximity to actual critical infrastructure. Exercises showcasing military and civilian response capabilities serve as a deterrent for possible adversaries.

The DOD should permanently assign a joint force to USNORTHCOM that is tasked organized to accomplish HD tasks. Even though the counter argument to an assigned force is the capability already resides across the joint services, this paper

argues that a permanently assigned HD response force provides more options to the Commander, USNORTHCOM. An assigned force builds a stronger rapport with inter agency partners, develops long term continuity, and focuses on current and emerging threats. An assigned response force offers the Commander, USNORTHCOM flexible deterrent and flexible response options while conducting HD. An HD response force should be separate from DSCA elements in case HD and DSCA missions occur simultaneously.

The actual size and composition of a permanent force requires a greater analysis than this paper offers. With that said, the HD response force requires sufficient capability to respond quickly, defend a critical site, and defeat conventional and asymmetrical threats up to a company size element. The HD response force must have the capacity to liaison with multiple civilian and interagency counterparts, and offer technical and tactical advice on defense of critical infrastructure. A permanently assigned force should consist of a command and control element, maneuver element, logistics element, and liaison element.

Joint interagency exercises should focus on plausible threat scenarios to rehearse unity of effort actions and employment of HD response forces. In addition to current threats, the military should focus table top exercises on future emerging threats to the homeland. Future exercises determine new threats, identify current gaps in interagency planning and interoperability, and drive future technology and equipment acquisitions. To keep pace with emerging threats to the homeland, new technology and equipment acquisitions should be planned several Program Objective Memorandum

cycles ahead of the anticipated threat. HD procurements and acquisitions should be a priority for the joint force.

Continued partnership must be a priority for the DOD. The military should pursue aggressive leader development programs focused on HD and interagency coordination. HD talent development and management should include multiple broadening experiences and interagency exchanges to build career long rapport among tactical, operational, and strategic leaders. The experience gained from these exchanges builds generational experience for the force and will pay lasting dividends in cooperation and collaboration. Leaders who participate in interagency exchanges should be assigned to USNORTHCOM for a utilization tour.

The balancing act of HS support and HD should constantly be assessed. What are the triggers that pushes an event to a HD operation or a HS operation? With today's asymmetrical threats and the low possibility of a conventional uniformed adversary, it is important to identify the thresholds that constitute an attack requiring military response. Intelligence that identifies a pending attack may be the prelude to an active presence of military power as part of the CIP.

Exercises should test these boundaries and establish clear demarcation points of authority. With growing threats, it is critical that changes in the lead and supporting agency process is codified either through policy, memorandums of understanding and/or agreement. The DOD and DHS must exercise, on a reoccurring cycle, transitioning from lead agency to supporting agency when actual threats or actions move from the HS to HD realm or vice versa.

Conclusion

Trust in the U.S. military's ability to protect the homeland is vital to ensuring America's national interests are protected. To keep America's trust the government must ensure America is protected at home by establishing effective defensive measures. Quality defensive measures increase critical infrastructure protection, thereby preserving the chances of economic stability and a fruitful American way of life.

In the future, the U.S. may face competing complex dilemmas that create unique challenges for the military and other agencies. HD and HS operations require a whole of government approach, among the multiple stakeholders, to ensure the continued protection of America's homeland and the nation's critical infrastructure. Continued investment of time and resources is required to ensure that the U.S. Government meets these challenges. The DOD and DHS must continue to work together by sharing intelligence, conducting exercises, and war gaming multiple worse case scenarios.

This paper has shown that protecting the nation's critical infrastructure is vital to national security. A viable CIP takes the resources, cooperation, and collaboration of numerous agencies and departments. The paper has described several threat scenarios on key infrastructure that, if carried out, would have devastating effects on the nation's economy and national security. It takes a team effort to protect the nation's infrastructure. Only through a team effort can we make the nation safer and ensure America's prosperity and way of life.

Endnotes

[1] President Barack Obama, "Presidential Proclamation—Critical Infrastructure Security and Resilience Month, 2014," Presidential Proclamation, Washington, DC October 31, 2014.

[2] Military forces meaning all branches of service to include the Reserve and National Guard components.

[3] The White House, *Presidential Policy Directive 21-Critical Infrastructure Security and Resilience*, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, (accessed March 7, 2015).

[4] Ibid.

[5] Ibid.

[6] Barack H. Obama, *National Security Strategy*, (Washington, DC: The White House, February 2015), 2.

[7] Ibid., 7.

[8] Ibid., 2.

[9] Ibidl, 7.

[10] U.S. Joint Chiefs of Staff, *Homeland Defense,* Joint Publication 3-27 (Washington, DC: U.S. Joint Chiefs of Staff, July 29, 2013), x.

[11] Ibid.,vii.

[12] Ibid.,, II-1 thru II-2.

[13] Charles D. Hagel, *Quadrennial Defense Review,* (Washington, DC: U.S. Department of Defense, March 2014), 58.

[14] U.S. Joint Chiefs of Staff, JP 3-27, viii.

[15] *The Department of Homeland Security Mission Homepage*, http://www.dhs.gov/our-mission (assessed March 6, 2015).

[16] *The Department of Homeland Security Enterprise Homepage*, http://www.dhs.gov/homeland-security-enterprise-overview, (accessed March 15, 2015).

[17] U.S. Joint Chiefs of Staff, JP 3-27, vii.

[18] *Department of Homeland Security What is Critical Infrastructure Homepage*, http://www.dhs.gov/what-critical-infrastructure, (accessed February 28, 2015)

[19] *Department of Homeland Security and Resilience Homepage*, http://www.dhs.gov/what-security-and-resilience, (accessed on 6 March, 2015).

[20] U.S. Joint Chiefs of Staff, JP 3-27, III-20.

[21] Ibid., III-20.

[22] Ibid.

[23] Ibid., GL-8.

[24] The White House, *Presidential Policy Directive 21*.

[25] The Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, (Washington DC: Department of Homeland Security, 2013), 3.

[26] The White House, *Presidential Policy Directive 21*.

[27] Ibid.

[28] Ibid.

[29] Department of Homeland Security, Defense Industrial Base Sector Overview http://www.dhs.gov/defense-industrial-base-sector, (accessed February 28, 2015).

[30] Department of Homeland Security, *Defense Industrial Base Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan 2010*, http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base-2010.pdf (accessed March 15, 2015), iii.

[31] Department of Homeland Security, *What is Critical Infrastructure Homepage.*

[32] General Charles H. Jacoby, Jr. *A Statement on the Posture of United States Northern Command and North American Aerospace Defense Command,* Presented to Senate Armed Services Committee, (Washington DC: March 13, 2014), 13.

[33] Admiral M.G. Mullen, *The National Military Strategy of the United States of America,* (Washington DC: 2011), 10.

[34] Admiral William E. Gortney, *A Statement on the Posture of United States Northern Command and North American Aerospace Defense Command,* Presented to Senate Armed Services Committee, (Washington DC: March 12, 2015), 6.

[35] U.S. Department of Energy, *Large Power Transformers and the U.S. Electric Grid, Infrastructure Security and Energy Restoration*, http://energy.gov/sites/prod/files/Large%20Power%20Transformer%20Study%20-%20June%202012_0.pdf (accessed March 5, 2015), 7.

[36] Ibid.

[37] Ibid., 5.

[38] Ibid., 1.

[39] Ibid., 9.

[40] Ibid.

[41] Ibid., 22.

[42] Clay Wilson, *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments,* (Washington, DC: U.S. Library of Congress, Congressional Research Service, July 21, 2008), 5.

[43] Ibid., 20.

[44] Ibid., 10.

[45] Ibid., 11.

[46] Ibid.

[47] Ibid., 12.

[48] Ibid.

[49] Cynthia E. Ayers and Kenneth D. Chrosniak, "Terminal Blackout: Critical Electric Infrastructure Vulnerabilities and Civil-Military Resiliency," Issue Paper, Center of Strategic Leadership and Development, U.S. Army War College, Volume 1-13, (October 2013) http://www.csl.army.mil/usacsl/publications/IP_1-13-Critical_Electric_Infrastructure.pdf (accessed March 18, 2015), 4.

[50] U.S. Congress, House of Representatives, Committee on the Armed Services, *The National Defense Authorization Act for Fiscal Year 2014 and Oversight of Previously Authorized Programs on the postures of U.S. Northern Command and U.S. Southern Command: Hearings before the Committee on Armed Services House of Representatives*, 113th Cong., 2nd sess., Full committee hearing, March 20, 2013, 35.

[51] Wilson, *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices,* 17.

[52] Gortney, *A Statement on the Posture of United States Northern Command and North American Aerospace Defense Command,* 6.

[53] Wilson, *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments,* 1.

[54] The White House, Presidential Policy Directive 21

[55] Jeh Charles Johnson, *Quadrennial Homeland Security Review*, (Washington, DC: U.S. Department of Homeland Security, June 2014) 28.

[56] Department of Homeland Security website, http://www.dhs.gov/transportation-systems-sector, accessed 7 March 2015.

[57] Department of Homeland Security, *Small Vessel Security Strategy*, (Washington, DC: The Department of Homeland Security, April 2008), http://www.dhs.gov/xlibrary/assets/small-vessel-security-strategy.pdf, (accessed March 18, 2015), 4.

[58] John F. Frittelli, *Port and Maritime Security: Background and Issues for Congress* (Washington, DC: U.S. Library of Congress, Congressional Research Service, May 27, 2005), 5.

[59] Department of Homeland Security, *Small Vessel Security Strategy*, 10.

[60] Ibid., 8.

[61] Ibid.,10.

[62] Frittelli, *Port and Maritime Security: Background and Issues for Congress*, 5.

[63] Ibid.

[64] Ibid., 5-6.

[65] U.S. Joint Chiefs of Staff, JP 3-27, II-18.

[66] Gortney, *A Statement on the Posture of United States Northern Command and North American Aerospace Defense Command*, 12.

[67] Leon E. Panetta, *Strategy for Homeland Defense and Defense Support of Civil Authorities,* (Washington, DC: U.S. Department of Defense, February 2013), 1.

[68] Johnson, *Quadrennial Homeland Security Review*, 18.

[69] Ibid., 29.

[70] U.S. Joint Chiefs of Staff, JP 3-27, I-2.

[71] USNORTHCOM vision. http://www.northcom.mil/Newsroom/FactSheets/ArticleView/tabid/3999/Article/563996/usnorthcom-vision.aspx, (accessed 27 February 2015).

[72] Gortney, *A Statement on the Posture of United States Northern Command and North American Aerospace Defense Command*, 3.

[73] U.S. Joint Chiefs of Staff, JP 3-27 (Washington, DC: U.S. Joint Chiefs of Staff, ix.

[74] Jacoby, *A Statement on the Posture of United States Northern Command and North American Aerospace Defense Command*, 2.

[75] Ibid., 3.

[76] USNORTHCOM vision.

[77] U.S. Congress, *The National Defense Authorization Act for Fiscal Year 2014 and Oversight of Previously Authorized Programs on the postures of U.S. Northern Command and U.S. Southern Command,* 57.

[78] U.S. Joint Chiefs of Staff, JP 3-27, II-21.

[79] Admiral M.G. Mullen, *The National Military Strategy of the United States of America,* (Washington DC: 2011), 10.

[80] Hagel, *Quadrennial Defense Review 2014*, 53-54.

[81] Testimony by General Jacoby to the Senate Armed Services Committee on March 13, 2014, 6.

[82] Robert M. Gates, *Ballistic Missile Defense Review Report*, (Washington, DC: Department of Defense, February 2010), 4.

[83] Jacoby, *A Statement on the Posture of United States Northern Command and North American Aerospace Defense Command*, 7.

[84] Ibid., 8.

[85] Robert M. Gates, *Ballistic Missile Defense Review Report*, (Washington, DC: U.S. Department of Defense, February2010), http://www.defense.gov/bmdr/docs/BMDR%20as%20of%2026JAN10%200630_for%20web.pdf, (accessed March 18, 2015), 11.

[86] Ibid.